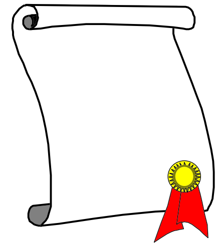
CRL Modeling

David A. Cooper
NIST



September 10, 1998

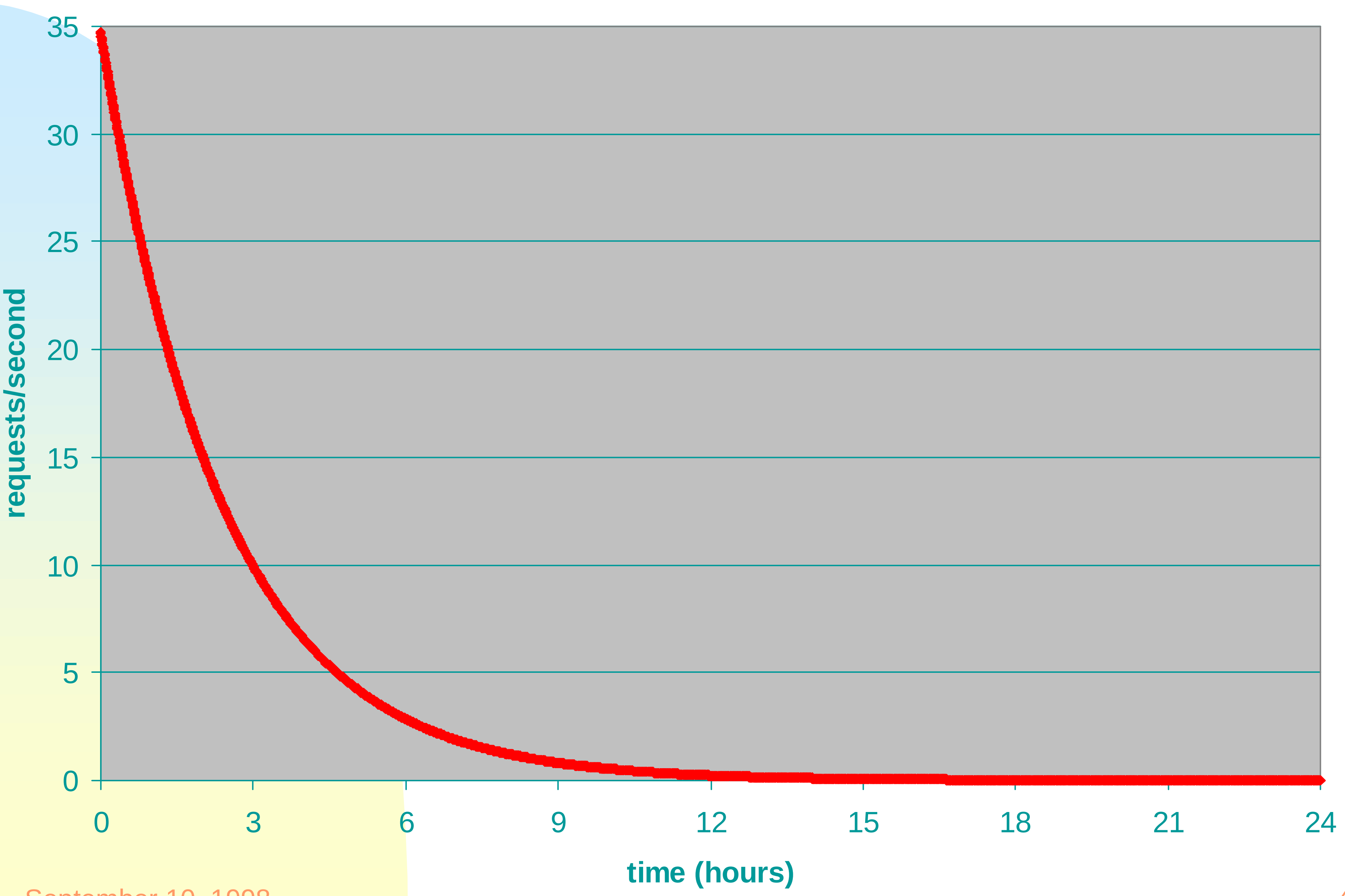
Repositories

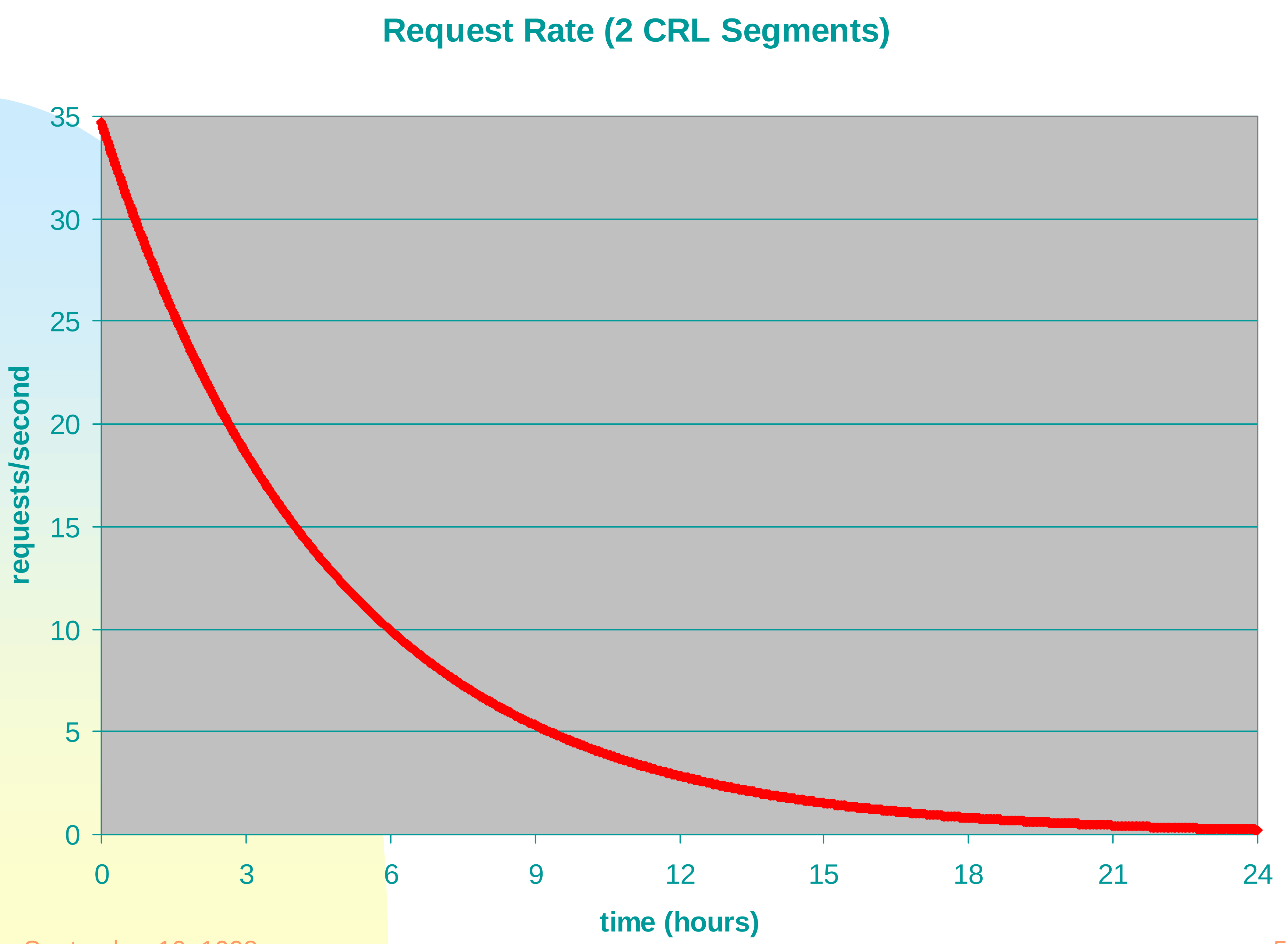
- Goal of work is to examine effect of different CRL schemes on repositories.
- Assumption: The main concern is to minimize the peak load on a repository.
  - Allows use of least expensive repository; or
  - maximizes number of relying parties that can be serviced.

Request Rates

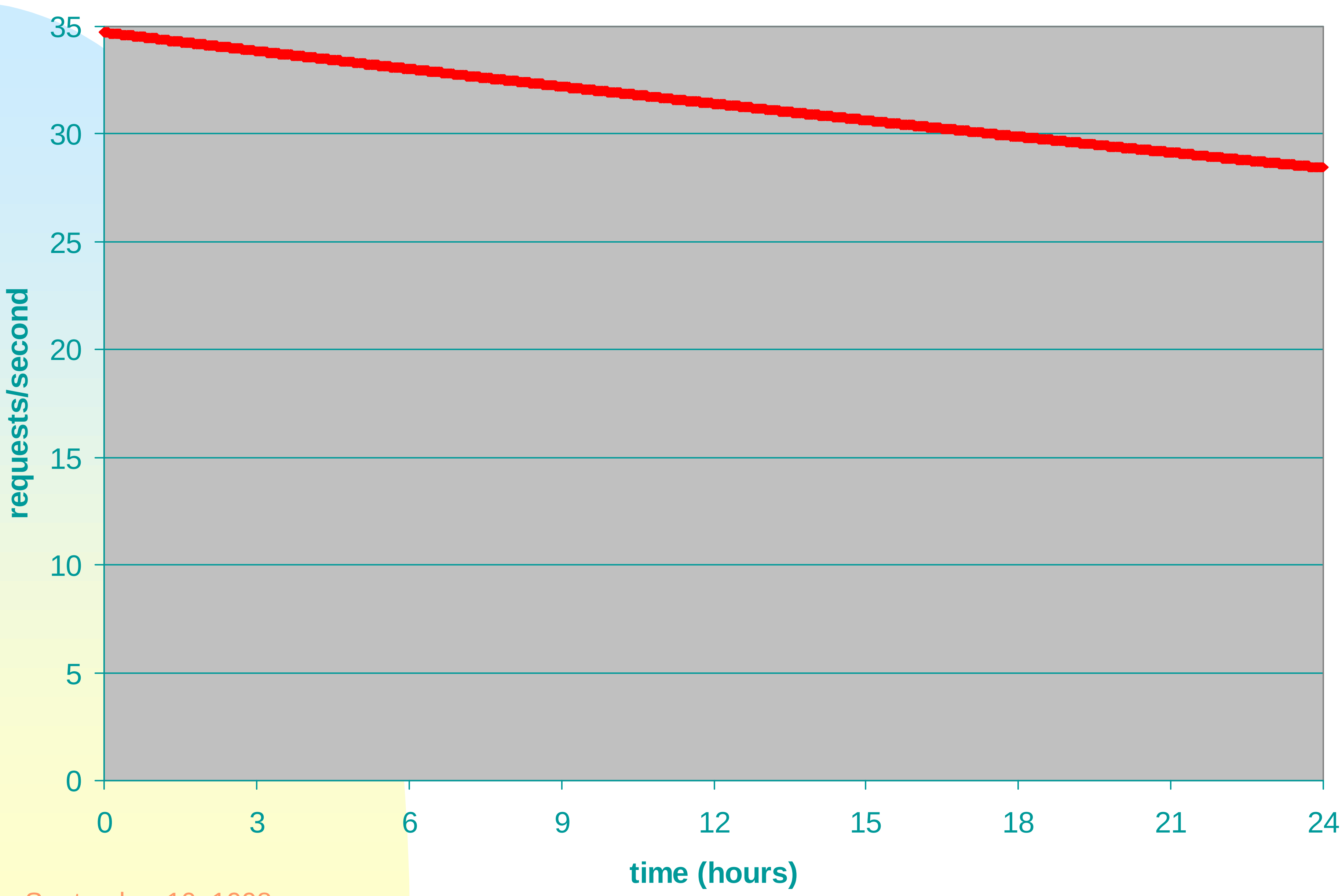
- n = Number of relying parties: 300,000
- v = validation rate: 10 certificates/relying party/day
- u = Revocation updates: 1 update/day
- s = number of segments
- t = amount of time since last CRL update
- request rate per segment= $(n\ v\ /\ s)\ e^{-v\ t\ /\ s}$
- peak request rate = $n\ v$

Request Rate (Unsegmented CRL)




Request Rate (2 CRL Segments)
requests/second
35
30
25
20
15
10
5
0
0
3
6
9
12
15
18
21
24
time (hours)

Request Rate (50 CRL Segments)

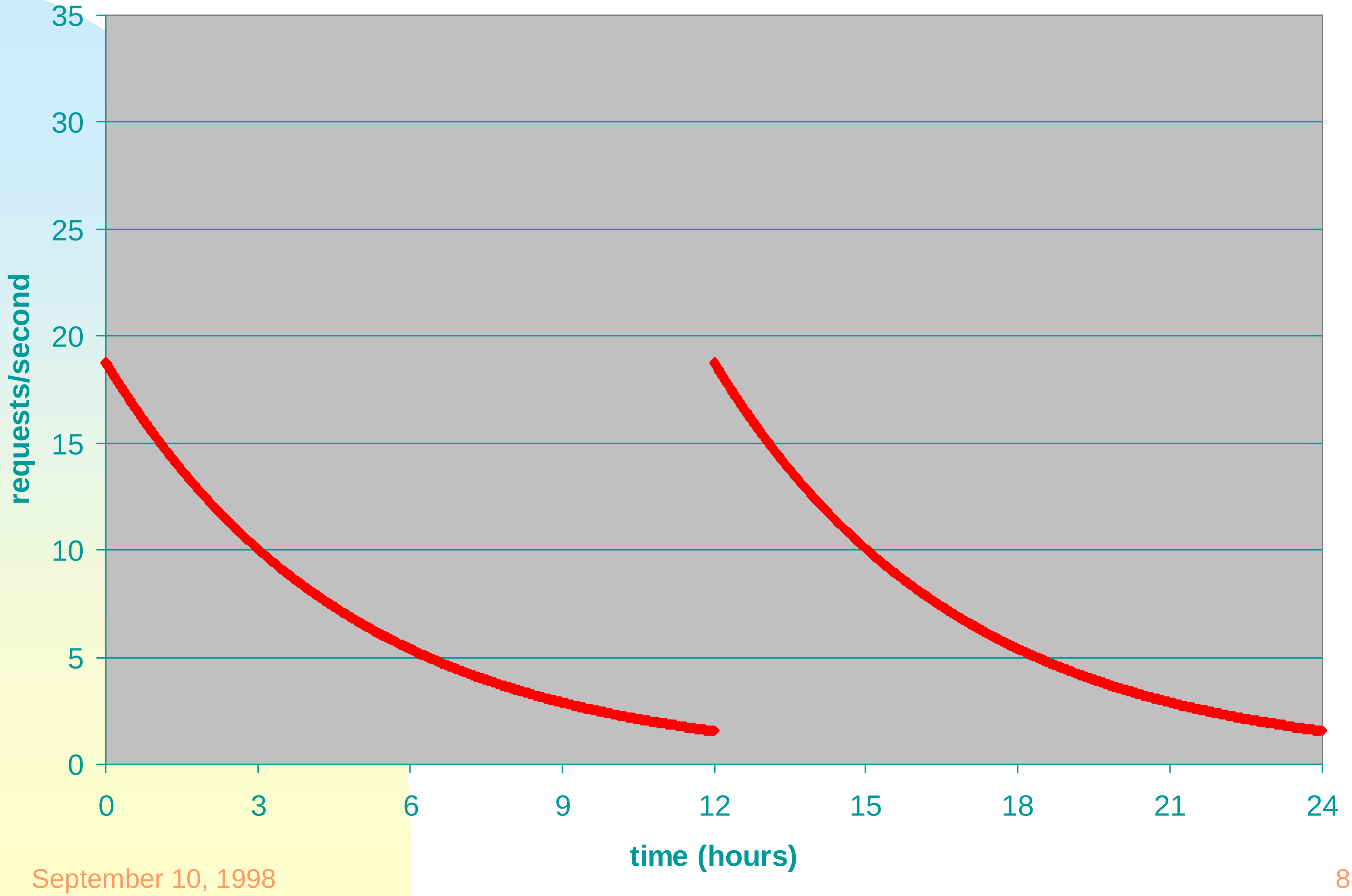


Staggered CRL Issuance

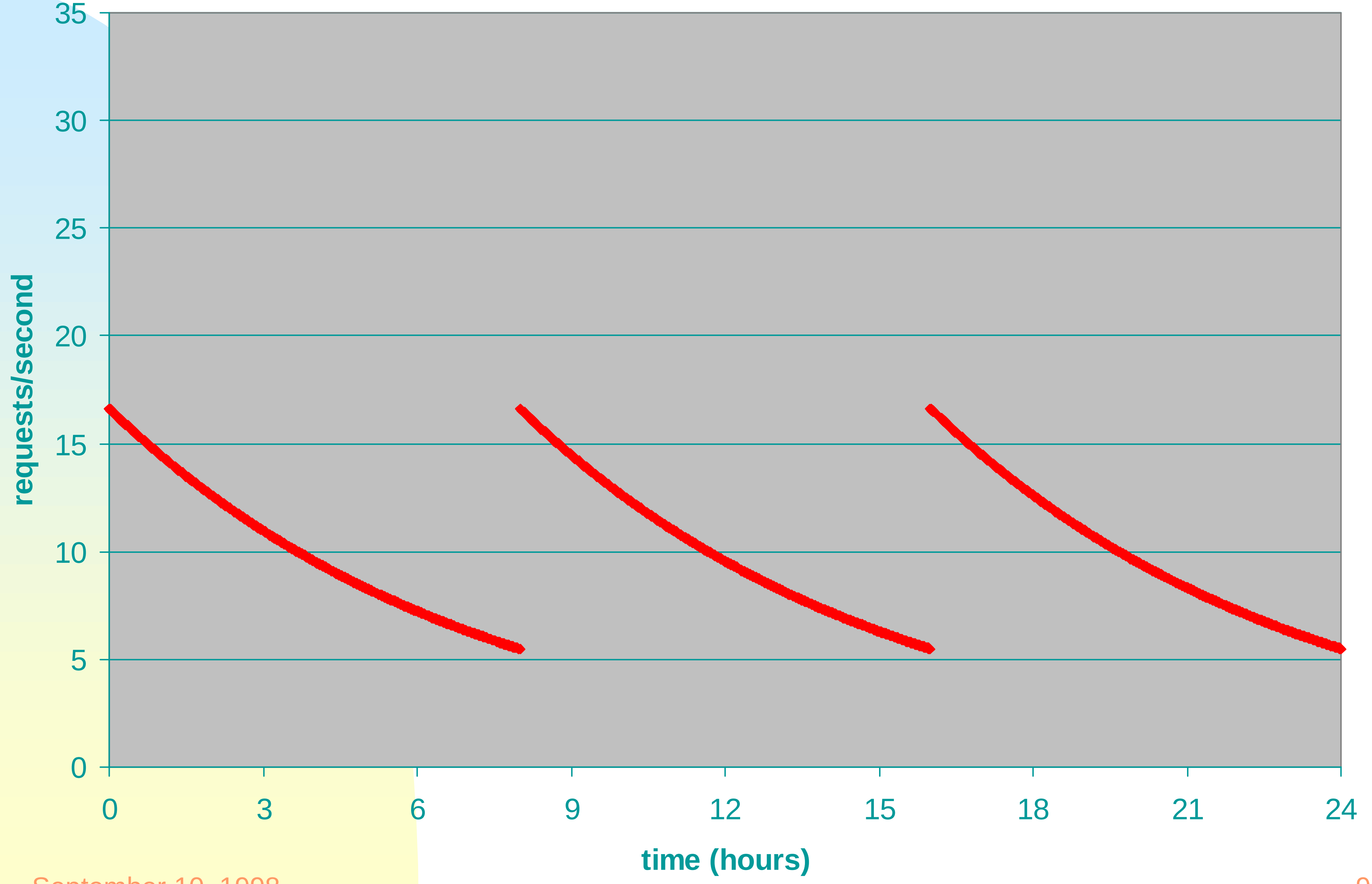
- CRL segments don’t have to be issued simultaneously
- 2 CRL segments issued at 12 hour intervals leads to lower peak request rate
- request rate (for 2 CRL segments) =

$$(n\ v / s)\ (e^{-v\ t / s} + e^{-v(t+12) / s})$$

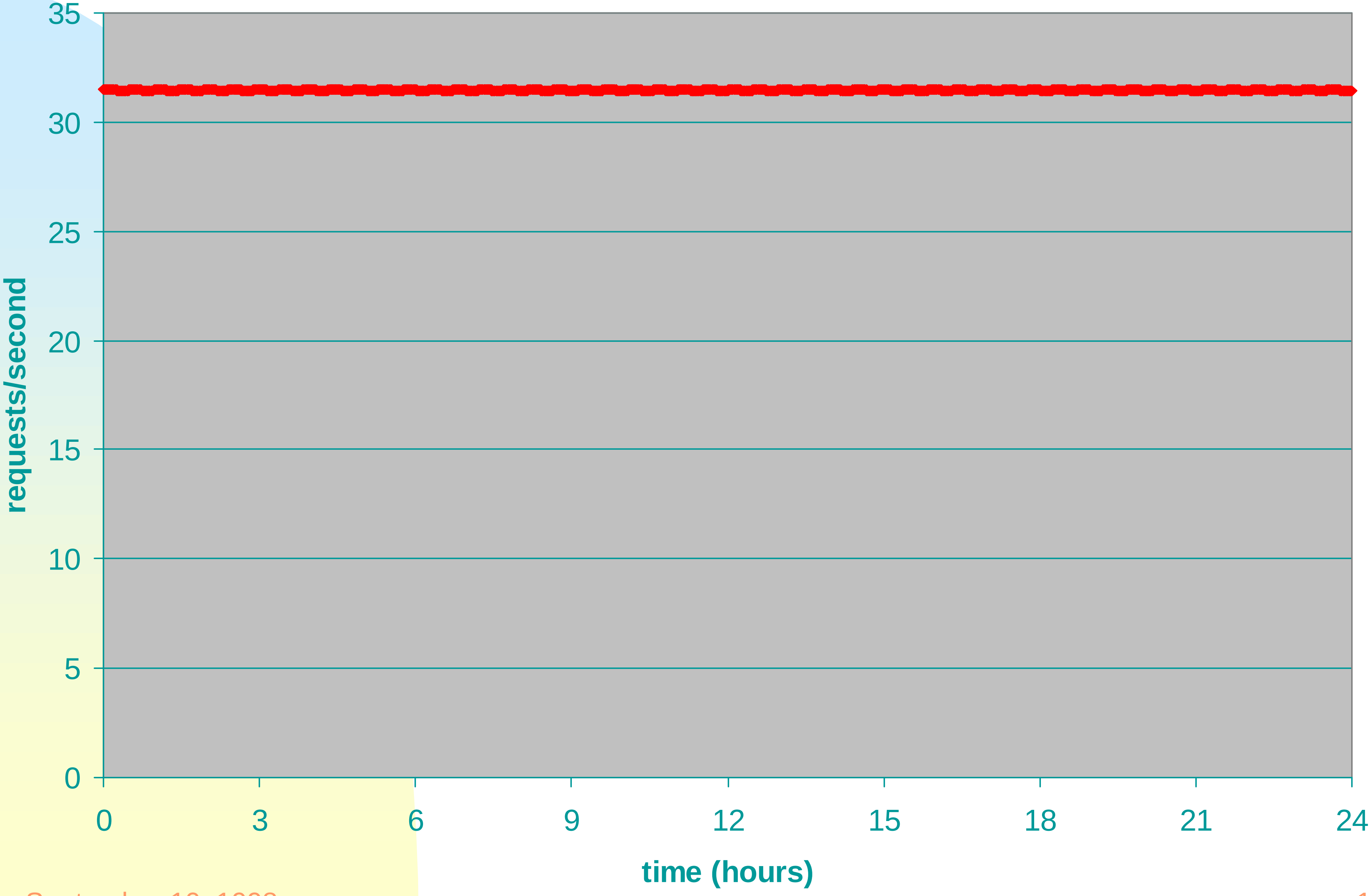
Request Rate (2 CRL Segments- Staggered Issuance)



Request Rate (3 CRL Segments - Staggered Issuance)



Request Rate (50 CRL Segments- Staggered Issuance)

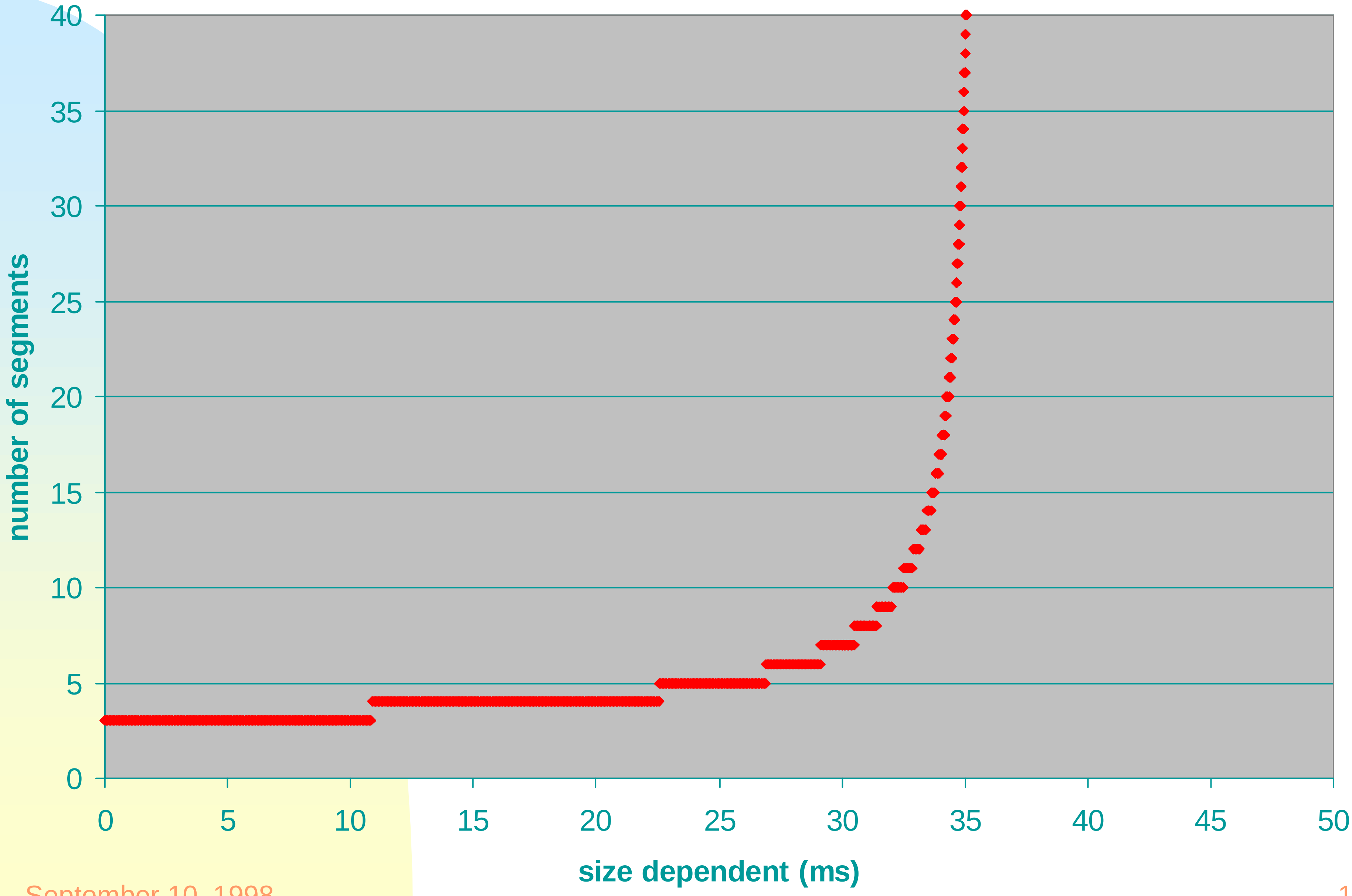


Service Rate

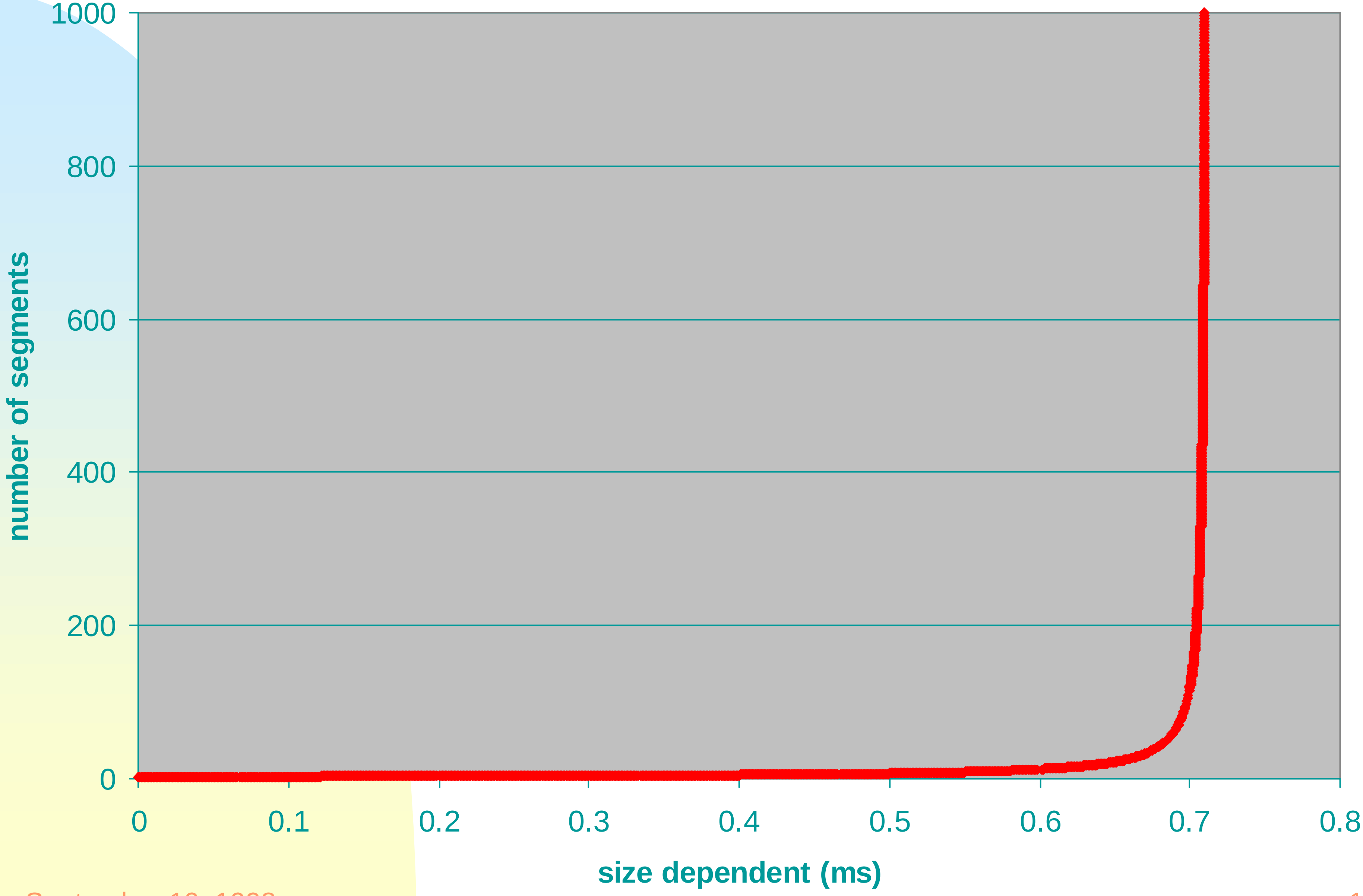
- Larger CRL segments may reduce request rate, but may also reduce service rate.
- If λ = request rate and μ = service rate:
  - average waiting time $\cong 1 / (\mu - \lambda)$
- Service time increases linearly with CRL segment size =

  Header + (# entries)(per entry cost)
- Less segmentation better when fixed cost dominates.

Optimal Segmentation (1 day)

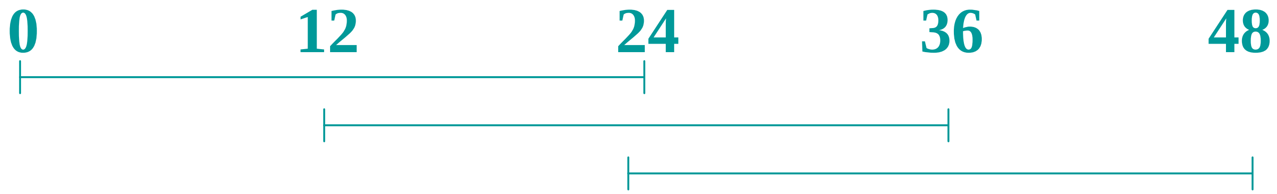


Optimal Segmentation (10 minutes)

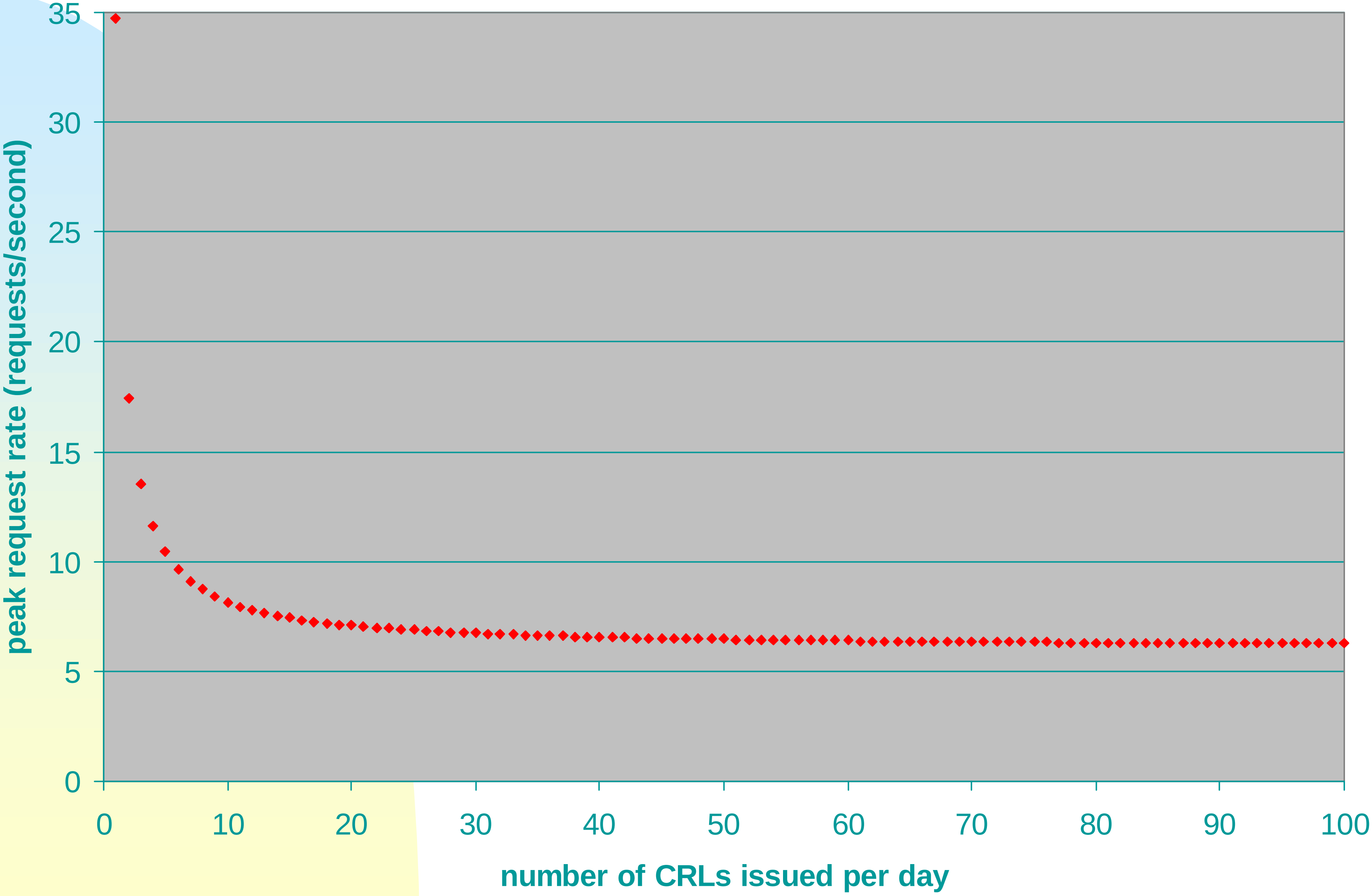


Over-issued CRLs

- Issue full CRLs more than once per day
- Make each CRL valid for one day
- Improves use of caches
- Spreads out CRL requests



Over-Issued CRLs



Questions

- What are the most important parameters?
  - Mean waiting time per request? (peak or average)
  - Mean total waiting time? (i.e., average total waiting time per relying party per day)
  - Peak bandwidth requirements?
  - Average bandwidth requirements?
  - Cache size?
  - Others?